Casa di Ricovero "Muzan"

Malo (V I)

Documento Programmatico sulla sicurezza

INDICE

1 DESCRIZIONE DEL SISTEMA INFORMATICO AZIENDALE

Il capitolo rappresenta gli elementi fondamentali del sistema informatico della **Casa di Ricovero "Muzan" di Malo (VI)**, con particolare riguardo agli aspetti hardware e ai collegamenti esistenti con le varie strutture aziendali.

In particolare è descritta l'architettura del sistema, individuandone gli elementi rilevanti ai fini della sicurezza informatica.

1.1 Struttura Fisica

La **Casa di Ricovero "MUZAN"** ha sede a Malo (VI), in Via Barbè 39, ed opera su una rete aziendale così strutturata:

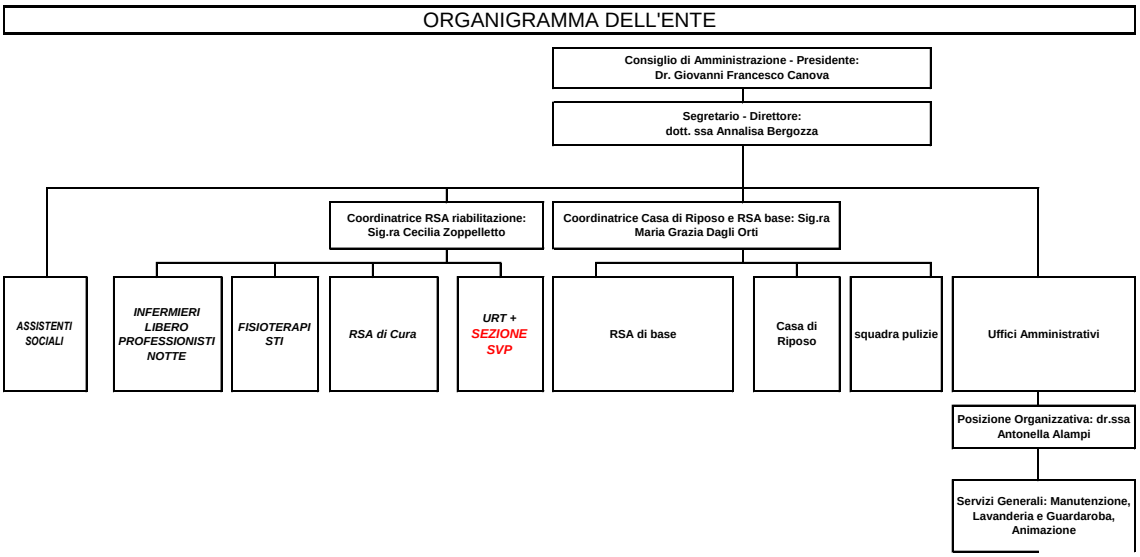
- 1 Server di dominio Windows 2003 Server S.P.2 (HP Proliant ML310) che opera anche come file server;
- 1 Firewall Watchguard X550E;
- 1 Proxy GFI Webmonitor, che filtra e controlla l'intero traffico internet (da interno verso esterno);
- 1 Router LinkSys X300 utilizzato per la connessione ADSL con NGI (internet);
- 1 Router CISCO 800 utilizzato per la connessione alla rete dell'ULSS4;
- 15 Client circa;
- Antivirus Trend Micro Worry-free Business Security, installato sul server ed in cascata sui clients (Trend Micro Officescan);
- 1 NAS su Terastation, connessa via rete, utilizzata per il backup dei dati.
- Impianto di videosorveglianza, con 8 postazioni distribuite tra interno ed esterno delle 3 strutture; registrazione "on-motion" su hard-disk con durata media 48/72 ore.

1.2 Organigramma Aziendale

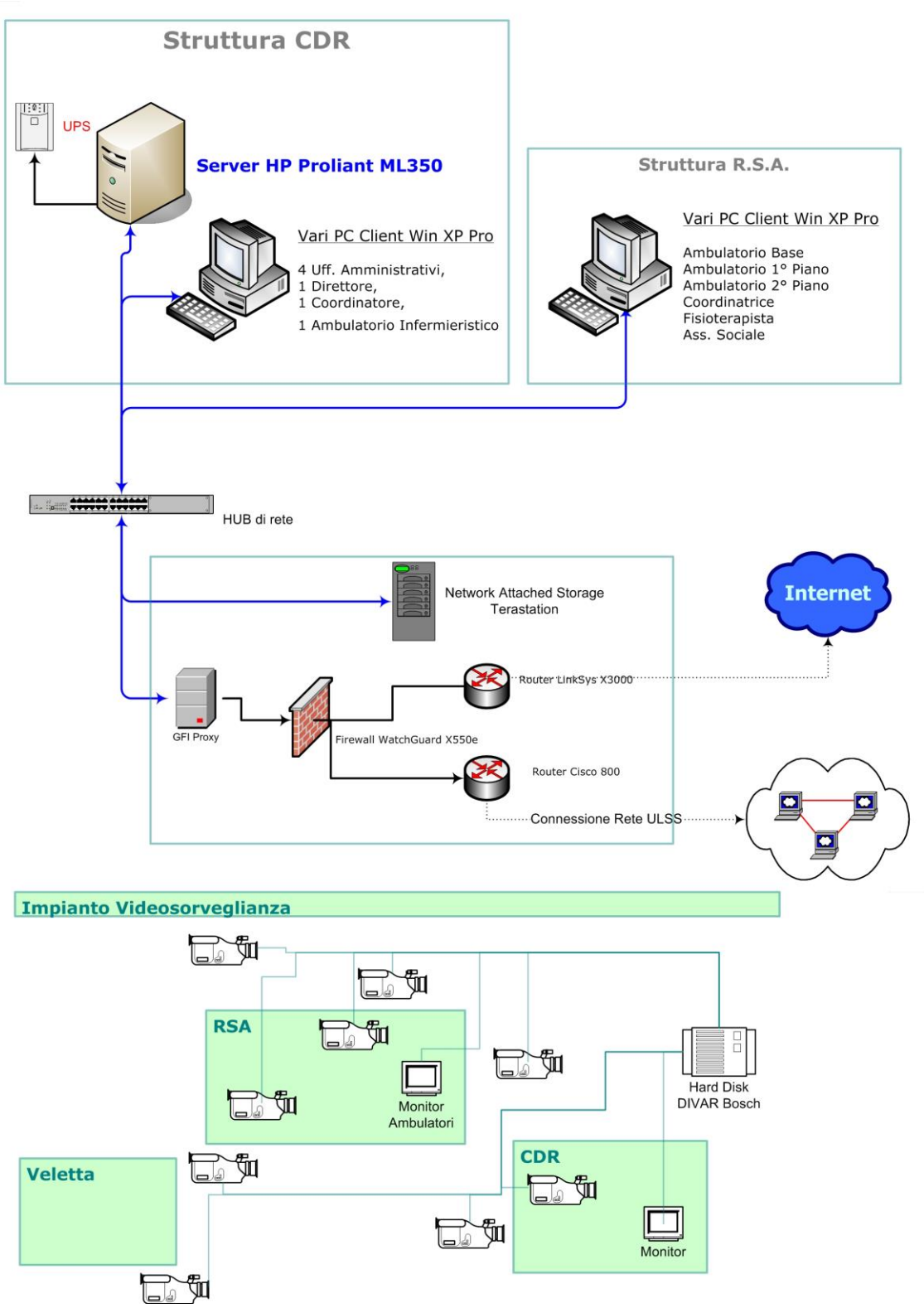
La casa di Ricovero "Muzan" opera nel campo dei servizi sociali e socio-sanitari, offrendo assistenza a persone adulte ed anziane, su una struttura composta da:

- Una casa di Riposo, per gli ospiti residenziali;
- Il nucleo RSA di base, nel quale vengono accolti gli ospiti non deambulanti o con particolari necessità assistenziali, in lista d'attesa di essere accolti nella casa di riposo;
- Il nucleo RSA riattivativo, al primo piano, nel quale sono accolti pazienti di provenienza dai vari reparti delle strutture ospedaliere territoriali, per processi di riabilitazione;
- Il nucleo RSA al secondo piano (in trasformazione da Residenza Sanitaria Assistenziale, a URP Unità Riabilitativa Territoriale), che accoglie pazienti esclusivamente dai reparti ospedalieri di ortopedia e neurologia.

Nel prospetto che segue è riportata in linea generale la struttura organizzativa della Casa di Ricovero: i nominativi delle figure professionali che operano in Istituto sono elencate nella pianta organica a disposizione presso l'ufficio Gestione Risorse Umane.



2 SCHEMA SINTETICO DELLA RETE AZIENDALE



3 ANALISI DEI RISCHI E MISURE MINIME DI SICUREZZA

3.1 Premessa

L'analisi dei rischi, prevista al punto 19 del Disciplinare tecnico, costituisce la fase di partenza delle attività di definizione e attuazione della politica di sicurezza aziendale.

Per potere svolgere questa analisi sono state analizzate:

- le principali caratteristiche tecniche degli edifici e dei locali in cui sono localizzati gli strumenti elettronici, attraverso i quali si effettua il trattamento dei dati aziendali
- le caratteristiche tecniche degli strumenti elettronici presenti presso la struttura
- le banche dati che contengono dati comuni e/o sensibili

L'obiettivo dell'analisi dei rischi è di acquisire consapevolezza sul livello di esposizione al rischio del proprio patrimonio informativo, e nello stesso tempo, avere una mappa delle contromisure di sicurezza da realizzare, garantendo il rispetto delle prescrizioni e un livello minimo di protezione, attraverso l'adozione delle misure minime di sicurezza (come previsto dagli artt. 33-35 D.lgs 196/03, dal Disciplinare tecnico - allegato B, dall' art. 31 D.lgs 196/03), in relazione alle tipologie dei dati aziendali trattati, alle modalità di trattamento e agli strumenti utilizzati.

La Politica di Sicurezza si basa sull'adozione di misure di tipo fisico, logico e organizzativo, gestite dalle procedure aziendali inserite nel presente Documento Programmatico, e che sinteticamente consistono in :

- ✓ **sicurezza fisica** diretta a prevenire accessi fisici non autorizzati, danni o interferenze con lo svolgimento dei servizi IT e a proteggere le apparecchiature hardware da danni accidentali o intenzionali. Comprende anche la sicurezza degli impianti di alimentazione e di condizionamento, la manutenzione dell'hardware e la protezione da manomissioni o furti;

- ✓ **sicurezza logica** diretta alla protezione dell'informazione e di conseguenza di dati, applicazioni, sistemi e reti;

- ✓ **sicurezza organizzativa** diretta alla definizione di ruoli, compiti, responsabilità e procedure per regolamentare gli aspetti organizzativi della Politica di Sicurezza.

3.2 Metodologia di analisi

L'analisi dei rischi è effettuata sulla base delle linee guida per la definizione di un piano per la sicurezza dei sistemi informativi automatizzati elaborate dal CNIPA.

La valutazione del rischio è basata su considerazioni soggettive unitamente all'istituzione di una scala semiqualitativa che individuerà varie soglie di rischio. La scala individuata prevede questi indici di rischio:

Indice	Descrizione
Lieve (L)	Con questa soglia viene individuato un rischio molto basso che identifica una minaccia remota e comunque rapidamente reversibile od ovviabile.
Medio (M)	Con questa soglia viene individuato un rischio superiore al precedente identificante una minaccia remota ma i cui effetti non sono totalmente o parzialmente reversibili od ovviabili. In tale caso è già consigliabile pensare ad accorgimenti per contenere il rischio.
Alto (A)	Con queste soglie viene individuato un rischio che è sicuramente inaccettabile pensare di correre, pertanto dovrà sicuramente essere attivato un insieme di contromisure (di natura fisica, logica, organizzativa) per abbattere il rischio e contenerlo a livelli accettabili.

Tabella 1

3.3 Analisi dei rischi sui luoghi fisici e misure di tipo fisico adottate

Rischio "Fisico"	Livello	Motivazione e misure adottate	Criticità / Misure adottate	Misure da adottare nell'ottica di un piano di miglioramento
Accesso non autorizzato ai locali **Sottrazione di strumenti contenenti dati**	Lieve	Al di fuori dell'orario, gli uffici amministrativi non sono accessibili in quanto chiusi a chiave. Dal momento che l'intero stabile è in ristrutturazione, è stato temporaneamente disdetto l'incarico di vigilanza precedentemente affidato alla società ProTecno Security di Schio. E' attivo inoltre un sistema di videosorveglianza: sono presenti 8 postazioni, dislocate internamente in prossimità degli ingressi, ed esternamente agli ingressi e nella zona retrostante della struttura. La registrazione viene effettuata su hard-disk DIVAR Bosch, ciclicamente, con durata di 48/72 ore : le registrazioni possono essere visualizzate via software dalle postazioni del Direttore e della Responsabile uffici amministrativi. Presso ciascun ambulatorio della struttura RSA, esiste un monitor che visualizza in tempo reale quanto avviene in corrispondenza di tutte le postazioni. Nessun allarme perimetrale è presente sia esternamente all'Istituto che negli uffici.	Il sistema di videosorveglianza prevede la registrazione per un tempo medio dalle 48 alle 72 ore, per una misura eccedente quindi rispetto a quanto previsto dal provvedimento del Garante.	
Allagamento	Lieve	Area non soggetta ad inondazioni o calamità di questo tipo.		

Rischio "Fisico"	Livello	Motivazione e misure adottate	Criticità / Misure adottate	Misure da adottare nell'ottica di un piano di miglioramento
Incendio	Lieve	Ogni locale di ciascuna sede è dotato di estintori per la soppressione dei focolai di incendio. L'Istituto hanno inoltre formulato un piano antincendio a cura del responsabile della sicurezza, con la formazione di risorse specifiche in questo ambito, in linea con quanto previsto dal D.Lgs. 81/08.		
Accesso non autorizzato **Furto di dati**	Lieve	Custodia degli archivi cartacei	Tutti i documenti cartacei contenenti dati personali / sensibili sono conservati in armadi chiusi a chiave o in uffici chiusi a chiave. Gli incaricati potranno prelevare i documenti necessari per il trattamento per il tempo necessario a tale operazione dopo di che avranno il compito di riporli nei luoghi preposti alla loro conservazione. Sarà compito dell'incaricato che preleva i documenti garantire che questi ultimi siano rinchiusi, sotto chiave, nel periodo di temporanea assenza dal posto di lavoro. Nel caso in cui l'ospite debba uscire dalla struttura per accertamenti o ricoveri, viene effettuata una copia di alcuni documenti (frontespizio della cartella con i dati riepilogativi dell'ospite; scheda terapia; referti se necessario; lettera di dimissione dall'ospedale, per gli ospiti della RSA) e trasmessi alla struttura che accoglie temporaneamente l'ospite. Al ritorno nella maggior parte dei casi la documentazione in copia viene inserita in cartella ospite, o distrutta con gli appositi	Nel caso in cui documenti riportanti dati sensibili o giudiziari debbano essere distrutti. Il diario clinico e le altre cartelle contenenti dati sanitari degli ospiti devono essere accessibili al solo personale incaricato: rimanendo responsabilità del soggetto titolare del dato (ovvero l'Istituto) definire criteri e modalità di trattamento dei dati personali, inclusi quelli idonei a rivelare lo stato di salute, annotati dal personale medico, è auspicabile la definizione di una procedura di accesso a tali dati, che ne garantisca la miglior acquisizione possibile in funzione delle necessità immediate dell'ospite e inibisca contestualmente l'accesso a dati non pertinenti o non necessari all'operatore che ne chiede la visione.

Rischio "Fisico"	Livello	Motivazione e misure adottate	Criticità / Misure adottate	Misure da adottare nell'ottica di un piano di miglioramento
			distruggi-documenti. Le schede terapia vengono mensilmente eliminate, in quanto la scheda viene ristampata: non è necessario mantenere le schede precedenti, in quanto firmate digitalmente dal medico direttamente su procedura Ospiti Track.	

3.4 Analisi dei rischi sulle risorse hardware e misure di tipo logico adottate

Rischio "Hardware"	Livello	Motivazione e misure adottate	Criticità / Misure adottate	Misure da adottare nell'ottica di un piano di miglioramento
Uso non autorizzato dell'hardware / Manomissione – Sabotaggio	Lieve	L'utilizzo dell'hardware è soggetto all'uso di password: l'accesso alle risorse di rete avviene con autenticazione di utente di dominio. Le policy di sicurezza sono gestite dall'amministratore di sistema, e prevedono la richiesta di modifica automatica della password a cadenza trimestrale, con lunghezza minima di 8 caratteri e con memoria delle 2 password precedenti ed obbligo di utilizzo di password complesse. L' accesso alla stanza Server è controllato, alle risorse hardware accedono solo persone autorizzate, e la manutenzione è effettuata a tecnici di fiducia.		
Probabilità/ frequenza di guasto	Lieve	L'hardware acquistato è di qualità: per quanto riguarda il server, è stato stipulato un contratto di manutenzione e assistenza, al fine di ridurre al minimo il rischio di malfunzionamento, e le conseguenze in seguito a guasti od anomalie software.		
Intercettazione delle trasmissioni	Lieve	L'accesso ad internet è consentito su linea ADSL tramite router, con autorizzazione su proxy GFI e con regole su firewall watchguard X550e: le regole sul firewall e sul proxy sono gestite solo da operatori autorizzati.	La conservazione dei log di navigazione viene effettuata per la durata media di circa un anno, con registrazione a livello utente del traffico effettuato.	L'attività di analisi sull'operato dei lavoratori deve essere oggetto di contrattazione sindacale : provvedere in tal fine a sottoscrivere un accordo tra le parti, che tenga conto anche della navigazione internet.
Rischi connessi	Lieve	Il server dispone di gruppo di continuità		

Rischio "Hardware"	Livello	Motivazione e misure adottate	Criticità / Misure adottate	Misure da adottare nell'ottica di un piano di miglioramento
all'elettricità		APC2200 che fornisce energia di buona qualità (stabilizzazione) e impedisce l'improvvisa assenza di corrente elettrica. E' attivo inoltre un generatore di energia che interviene a copertura della linea di tutti gli edifici della struttura.		
Supporti di memorizzazione : utilizzo improprio e/o malfunzionamenti	Lieve	Su base giornaliera e mensile viene effettuato un backup su NAS esterno.		

3.5 Analisi dei rischi sulle risorse dati e misure di tipo logico adottate

Rischio "Dati"	Livello	Motivazione e misure adottate	Criticità / Misure adottate	Misure da adottare nell'ottica di un piano di miglioramento
Accessi esterni non autorizzati **Cancellazione non autorizzata o manomissione di dati**	Lieve	L'accesso alle risorse dati in formato elettronico avviene solo tramite gli elaboratori protetti da password (con utenti in dominio). L'accesso agli applicativi Sherpa (via Web), prevede 2 livelli di accesso successivi, con password complesse che variano a cadenza trimestrale. Per le applicazioni gestite da CBA, al software del personale si accede via web, con autenticazione di utente e password: l'accesso all'applicativo presenze CBA invece, prevede un filtro con utente e password, che viene sostituita manualmente ad opera degli operatori stessi. Per la gestione delle cartelle ospiti, si utilizza un software reso disponibile dall'ULSS4, con accesso in VPN. Ai vari archivi cartacei possono accedere solo i diretti incaricati che possiedono le chiavi degli armadi o degli uffici in cui sono custoditi dati sensibili.	A cadenza periodica viene effettuata una verifica delle utenze attive non più autorizzate (es. personale non più in servizio). Ogni operatore autorizzato ha una suo utente individuale: ad ogni nuovo assunto viene data una nuova credenziale d'accesso ed ogni cessazione viene comunicata dalla coordinatrici all'ULSS.	L'accesso al software gestionale dell'ULSS4 non prevede il cambio automatico della password di accesso : inviare una comunicazione agli uffici di competenza, al fine di sollecitare l'adozione di sistemi automatici di cambio password, a cadenza trimestrale.
Perdita di dati	Lieve	I dati residenti in locale (sul server) vengono salvati giornalmente su NAS; i dati del gestionale SHERPA invece sono accessibili solamente via Web, pertanto è demandato ad ESAKON l'onere di effettuarne il backup secondo modalità e tempi in linea con quanto previsto dal codice.		

Rischio "Dati"	Livello	Motivazione e misure adottate	Criticità / Misure adottate	Misure da adottare nell'ottica di un piano di miglioramento
Attacchi da virus	Lieve	Tutta la rete è protetta da software antivirus **Trend Micro Worry-Free Business Security** installato su server, che provvede al monitoraggio dei vari client, tramite apposito agent installato localmente (OfficeScan); la connessione ad internet è protetta da firewall e con regole su proxy.		
Intercettazione di informazioni in rete	Lieve	L'accesso ad internet è consentito su linea ADSL tramite autorizzazione su proxy GFI e firewall Watchguard: le regole sul firewall e sul proxy sono gestite solo da operatori autorizzati. Attualmente non sono attive connessioni VPN con nessuna fonte esterna.		
Accesso da Amministratore di Sistema	Lieve	Come da provvedimento del Garante del 27 novembre 2008, gli accessi da parte degli amministratori di sistema devono essere registrati in appositi LOG.	L'utente "administrator" di accesso privilegiato ai server, è utilizzato indistintamente da figure professionali diverse : l'azienda che si occupa della manutenzione dell'hardware sta provvedendo a distinguere nominalmente gli utenti con profilo di amministratore, al fine di avere la certezza di quale sia l'utente che realmente sta operando.	

3.6 Analisi dei rischi sulle risorse software e misure di tipo logico adottate

Rischio "Software"	Livello	Motivazione e misure adottate	Criticità / Misure adottate	Misure da adottare nell'ottica di un piano di miglioramento
Accesso non autorizzato alle basi dati connesse	Lieve	I software che trattano i dati controllano l'accesso tramite una finestra di autenticazione (finestra di Login). L'accesso agli altri software gestionali è garantito tramite autenticazione ed autorizzazione, e con profilo di autorizzazione specifico per singolo utente.		
Errori software che minacciano l'integrità dei dati	Lieve	I software sono utilizzati da tempo e non hanno mai causato la perdita o il danneggiamento dei dati trattati. Si veda inoltre quanto già riportato alla sezione "**Attacchi da virus**" riportata nel paragrafo relativo ai rischi sulle risorse dati.		
Presenza di un codice non conforme alle specifiche del programma	Lieve	I programmi sono forniti da produttori che operano nel settore con la massima serietà da molti anni, o creati da tecnici interni.		

3.7 Analisi dei rischi sulle risorse professionali e misure di sicurezza di tipo organizzativo adottate

Elemento di rischio	Livello	Motivazione e misure adottate	Criticità / Misure adottate	Misure da adottare nell'ottica di un piano di miglioramento
Errore materiale **Carenza di consapevolezza, disattenzione incuria**	Lieve	Sulla base dell'analisi dei rischi è stato redatto il presente Documento Programmatico sulla Sicurezza. Gli incaricati sono stati edotti sulle procedure messe in atto all' interno dell'azienda relativamente al trattamento dei dati personali, con appositi corsi di formazione interna. Le nomine a Responsabilità interna al Trattamento dei dati è stata effettuata a tutti i responsabili di area o servizio.		
Indisponibilità di accesso ai dati.	Lieve	Indicazione del custode delle copie delle credenziali di autenticazione.	E' stato individuato e nominato per iscritto la figura cui spetta la custodia, in un luogo sicuro, delle password degli utenti con accesso esclusivo (server, firewall, proxy; accesso a software con utente amministratore): rimane da verificare che le password siano effettivamente presenti e aggiornate.	
Accesso da Amministratore di Sistema	**Medio**	Come da provvedimento del Garante del 27 novembre 2008, devono essere individuate le figure che internamente, o per incarico esterno, accedono a sistemi e database con profilo di amministratore.	Le aziende che operano su hardware e software sono state designate come "Responsabile esterno al trattamento dei dati". Non è prevista internamente una figura che abbia mansioni e professionalità per assumere il ruolo di "Amministratore di Sistema"; un primo front-end per i problemi di natura informatica viene effettuato dalla responsabile servizi amministrativi, che poi provvede ad inoltrare la richiesta di intervento all'azienda che si occupa della manutenzione della rete.	Gli utenti che devono operare con profilo di amministratore non dispongono di un account specifico di accesso.

Elemento di rischio	Livello	Motivazione e misure adottate	Criticità / Misure adottate	Misure da adottare nell'ottica di un piano di miglioramento
Trattamento dati non conforme al codice	Lieve	Consegna del modello di clausola di "conformità" alle misure di sicurezza ad ogni intervento effettuato in via estemporanea da società o collaboratori, su server, hardware e software aziendali.	Nel caso in cui ci siano interventi da parte di aziende / professionisti, con i quali non sono in essere contratti di manutenzione annuale, e per i quali vi sia la necessità di accedere a server e/o a software che trattino dati personali / sensibili, si dovrà prevedere di far sottoscrivere al termine dell'intervento, un documento nel quale l'azienda / professionista dichiari che l'intervento effettuato è conforme alle disposizioni del Codice.	
	Lieve	Lettere di nomina a Responsabilità, attribuite dalla Casa di Ricovero alle terze parti.		Verificare che siano state attribuite dalla Casa di Ricovero le nomine a Responsabilità esterna, al fine di consentire il trattamento di dati di cui l'ente è Titolare (es. Società per i servizi di ristorazione, Cooperative per fornitura di servizi, etc).

4 CENSIMENTO ARCHIVI

	Gestione Segreteria	DOCUMENTI
BANCA DATI	Documento Excel contenente informazioni anagrafiche utili alla gestione amministrativa interna (protocollazione, redazione documenti).	Documenti realizzati con prodotti di office automation
Finalità del trattamento	Amministrativo.	Amministrativo
Tipo di Dati **(Personale / Sensibile / Giudiziario)**	**P**	**P**
Personale che ha accesso ai dati	Incaricate dell'ufficio Amministrazione.	Incaricate dell'ufficio Amministrazione.
Modalità di raccolta	Manuale, con documenti e modulistica.	Manuale, con documenti e modulistica.
Modalità di trattamento	Informatico, cartaceo	Informatico, cartaceo
Ambito di comunicazione	Ad uso esclusivamente interno.	Nessuno
Luogo in cui sono custoditi	Amministrazione	Vari uffici, ciascuno per i dati di sua competenza
Ubicazione (hardware)	Server 2012	Cartelle condivise su Server 2012
Tipo di connessione ai dati	Via rete locale LAN.	Via rete locale LAN
Misure di sicurezza adottate	Accesso al server protetto da password tramite autenticazione utente di sistema. Software Antivirus. Backup su Terastation.	Accesso protetto tramite autenticazione utente e password di sistema. Ciascun utente può accedere ad un insieme di cartelle così suddiviso: • Una propria cartella riservata; • Una cartella condivisa con un gruppo di lavoro (coordinatrici e amministrativi); • Una cartella pubblica, condivisa con tutti gli utenti. Backup su Terastation.
Annotazioni		

BANCA DATI	**Albo Pretorio On-Line** Pubblicazione su sito internet dell'Istituto della documentazione da esporre all'albo pretorio, come previsto da Legge 69 /2009: per la parte relativa agli atti amministrativi (delibere e determine), i testi pubblicati sono trattati in modo da eliminare i riferimenti o fatti riconducibili a persone.
Finalità del trattamento	Amministrativo
Tipo di Dati **(Personale / Sensibile / Giudiziario)**	**P**
Personale che ha accesso ai dati	Il dato è pubblicato manualmente sul sito internet www.muzan.it pertanto consultabile senza richiesta di autenticazione.
Modalità di raccolta	
Modalità di trattamento	Principalmente informatico.
Ambito di comunicazione	Il dato viene ovviamente diffuso su web.
Luogo in cui sono custoditi	Server del provider Tecnologie & Sistemi – Schio (VI)
Ubicazione (hardware)	Server farm del provider Tecnologie & Sistemi – Schio (VI)
Tipo di connessione ai dati	Via web
Misure di sicurezza adottate	L'accesso alla parte di amministrazione del sito è autorizzata esclusivamente ad un incaricato della Casa di Ricovero.
Annotazioni	

	SHERPA Contabilità Ospiti	SHERPA Contabilità
BANCA DATI	DataBase contenente informazioni relative agli ospiti, utili alla gestione anagrafica dello stesso (dati personali, dati dei familiari) e alla gestione della contabilità rette.	Database contenente informazioni relative ai clienti e fornitori, movimenti contabili, fatturazione.
Finalità del trattamento	Amministrativo, contabile.	Amministrativo, contabile.
Tipo di Dati (Personale / Sensibile / Giudiziario)	**P / S**	**P**
Personale che ha accesso ai dati	Incaricate dell'ufficio Amministrazione.	Incaricate dell'ufficio Amministrazione.
Modalità di raccolta	Manuale, con documenti e modulistica; via software, con recupero informazioni da Enti Esterni (ASL, Inps, etc).	Manuale, con documenti e modulistica.
Modalità di trattamento	Informatico, cartaceo	Informatico, cartaceo.
Ambito di comunicazione	Ad uso interno. Dati comunicati a strutture pubbliche (Enti Locali, Inps, ASL).	Ad uso interno. Dati comunicati a istituti previdenziali ,assistenziali, fiscali (Inps, Inail, , Agenzia Entrate, etc).
Luogo in cui sono custoditi	Amministrazione	Amministrazione
Ubicazione (hardware)	Server di Esakon – Trento.	Server di Esakon – Trento.
Tipo di connessione ai dati	Via Web, con accesso protetto alla rete Esakon, e ulteriore autorizzazione per accesso remoto protetto.	Via Web, con accesso protetto alla rete Esakon, e ulteriore autorizzazione per accesso remoto protetto.
Misure di sicurezza adottate	Accesso dai server di Esakon alla connessione remota sugli applicativi attivi per l'azienda (utente / password). Accesso alla base dati protetto da password tramite autenticazione utente di procedura. Ogni altra misura di sicurezza adottata da Esakon a protezione dei propri sistemi.	Accesso dai server di Esakon alla connessione remota sugli applicativi attivi per l'azienda (utente / password). Accesso alla base dati protetto da password tramite autenticazione utente di procedura. Ogni altra misura di sicurezza adottata da Esakon a protezione dei propri sistemi.
Annotazioni	Le password variano a cadenza trimestrale.	Le password variano a cadenza trimestrale.

	CBA Presenze	Gestione Stipendi
BANCA DATI	DataBase contenente informazioni relative alle presenze e assenze dei dipendenti e assimilati.	Informazioni relative ai dati economici ed anagrafici dei dipendenti, necessari e correlati alla produzione del cedolino paga e relative denunce mensili / annuali.
Finalità del trattamento	Amministrativo, contabile.	Amministrativo, contabile.
Tipo di Dati (Personale / Sensibile / Giudiziario)	**P / S**	**P / S**
Personale che ha accesso ai dati	Incaricate dell'ufficio Amministrazione. Coordinatrici, per gestione dei turni del personale.	Incaricate dell'ufficio Amministrazione.
Modalità di raccolta	Manuale, con documenti e modulistica.	Manuale, con documenti e modulistica.
Modalità di trattamento	Informatico, cartaceo	Cartaceo.
Ambito di comunicazione	Ad uso interno.	Ad uso interno : le elaborazioni avvengono presso la società CBA di Trento.
Luogo in cui sono custoditi	Amministrazione	Ufficio Ragioneria - Personale
Ubicazione (hardware)	Server 2003	
Tipo di connessione ai dati	Via rete locale LAN.	
Misure di sicurezza adottate	Accesso protetto da password tramite autenticazione utente di sistema e utente di procedura. Software Antivirus Trend Micro. Backup su Terastation.	Armadi dotati di serratura.
Annotazioni	La password di accesso variano a cadenza trimestrale, ad opera dei singoli utenti.	Dal marzo 2012 l'imputazione dei dati variabili mensili avviene tramite accesso web agli applicativi installati in sede CBA: al termine delle elaborazioni la società invia le stampe in formato pdf all'ufficio personale.

BANCA DATI	PA04 (Sonar) – INPDAP	Gedap
	DataBase contenente informazioni anagrafiche e previdenziali del personale dipendente	Database contenente deleghe sindacali.
Finalità del trattamento	Amministrativo, contabile.	Amministrativo.
Tipo di Dati (Personale / Sensibile / Giudiziario)	**P**	**P**
Personale che ha accesso ai dati	Incaricate dell'ufficio Amministrazione.	Incaricate dell'ufficio Amministrazione.
Modalità di raccolta	Manuale, con documenti e modulistica; via software, con recupero informazioni da Enti Esterni (INPDAP, etc).	Manuale, con documenti e modulistica.
Modalità di trattamento	Informatico, cartaceo	Informatico, cartaceo.
Ambito di comunicazione	Ad uso interno e dati comunicati a INPDAP.	Ad uso interno.
Luogo in cui sono custoditi	Amministrazione	Amministrazione
Ubicazione (hardware)	PC Ufficio Personale	PC Ufficio Personale
Tipo di connessione ai dati	In locale	In locale
Misure di sicurezza adottate	Accesso protetto da password tramite autenticazione utente di sistema e utente di procedura. Software Antivirus.	Accesso protetto da password tramite autenticazione utente di sistema e utente di procedura. Software Antivirus.
Annotazioni		

BANCA DATI	**Segreteria Ospiti** Documenti di office automation e documentazione cartacea, suddivisa tra fascicolo amministrativo (dati anagrafici dell'ospite e dei tutori o amministratori di sostegno, contratti o convenzioni riguardanti l'ospite), fascicolo sociale (schede SVAMA, documentazione prodotta da assistente sociale, report di unità operativa interna, colloqui sociali), diario clinico.
Finalità del trattamento	Amministrativo, sanitario.
Tipo di Dati **(Personale / Sensibile / Giudiziario)**	**P / S**
Personale che ha accesso ai dati	Amministrativi, operatori socio-assistenziali, personale infermieristico.
Modalità di raccolta	Manuale, con documenti e modulistica.
Modalità di trattamento	Cartaceo.
Ambito di comunicazione	Ad uso interno.
Luogo in cui sono custoditi	Armadi e schedari in ufficio Segreteria
Ubicazione (hardware)	
Tipo di connessione ai dati	
Misure di sicurezza adottate	La documentazione cartacea è riposta in un armadio chiuso a chiave in segreteria: l'ufficio è sempre presidiato, e viene chiuso a fine giornata.
Annotazioni	I dati storici sono in un'area all'ultimo piano della CDR. Nel caso di dimissione/ decesso di un ospite viene effettuata una copia cartacea di tutti i documenti della cartella (compresi referti, esami, etc) , e consegnati in originale ai familiari (ad eccezione del diario clinico e del diario delle consegne), unitamente alla lettera di dimissione della RSA e all'eventuale libretto di pensione consegnato al momento dell'ingresso. Nella cartella vengono raccolte anche tutti i documenti dei vari operatori (assistente sociale, educatrici, etc).

	Reparti – Cartella Ospiti	**IATROS**
BANCA DATI	Cartella contenente il "diario clinico", ovvero documento che riassume la storia e le necessità sia di carattere sanitario che assistenziale dell'ospite (compreso Piano assistenziale Individuale).	Anagrafica pazienti. Diario clinico: informazioni inerenti le diagnosi, le terapie ed altre informazioni di carattere sanitario.
Finalità del trattamento	Amministrativo, sanitario.	Amministrativo – Sanitario
Tipo di Dati **(Personale / Sensibile / Giudiziario)**	**P / S**	**P / S**
Personale che ha accesso ai dati	Medici, Infermieri.	Medico della CDR che tratta dati sensibili e personali.
Modalità di raccolta	Manuale, con documenti e modulistica.	Presso l'Ambulatorio in CDR. Manuale con documenti e modulistica.
Modalità di trattamento	Solamente cartaceo.	Informatico e cartaceo
Ambito di comunicazione	Ad uso interno.	Interno
Luogo in cui sono custoditi	Ambulatorio della struttura.	Singolo PC Ambulatorio CDR
Ubicazione (hardware)		Il software è installato in locale su PC e i dati sono salvati su server tramite un batch automatico.
Tipo di connessione ai dati	Schedari in ferro dotati di serratura, c/o ambulatorio.	Accesso in locale al software.
Misure di sicurezza adottate	All''ambulatorio di ciascun reparto (CDR e RSA 3 piani) vi accedono normalmente solo infermieri e medici (durante i turni di disponibilità): gli operatori non vi hanno accesso. Ogni ufficio è normalmente presidiato, in caso contrario è chiuso a chiave.	Accesso protetto da password tramite autenticazione utente/password di sistema e utente di procedura (ciascun medico utilizza un proprio account/password).
Annotazioni	Il diario clinico è normalmente consultato da infermieri e medico: agli operatori viene data visione solamente del Piano Assistenziale Individuale. Le analisi effettuate dai medici sono condivise con le informazioni raccolte dagli infermieri, attività necessaria vista la tipologia di struttura (non autosufficienti). Le schede terapia degli ospiti viene utilizzata durante tutta la giornata, e riposta a fine turno negli schedari nei vari ambulatori. Le chiavi a fine turno giornaliero, vengono consegnate all'infermiere del turno di notte.	

BANCA DATI	**Gestione Ospiti Track – ULSS 4** Gestione dati amministrativi, sanitari e socio-sanitari, degli ospiti accolti nelle varie strutture della casa di Ricovero. Il software è in gestione all'ULSS4, il quale ha reso disponibili una serie di postazioni di lavoro (2 in Amministrazione, 1 in RSA di base, 3 nelle RSA, 1 in CdR ed 1 presso l'Assistente Sociale), da cui si può accedere via VPN, su rete dedicata, al software installato presso i server dell'ULSS. Sono gestiti sia dati anagrafici dell'ospite, che dati sanitari (scheda terapia, con i dati dei vari farmaci; diario clinico del medico; diario infermieristico e schede bisogni) sia socio-sanitari (schede riabilitative di logopedisti e fisioterapisti; schede SVAMA; relazioni e valutazioni dei vari operatori tecnico-sanitari; documenti di analisi dell'Assistente Sociale).
Finalità del trattamento	Amministrativo, Contabile, Sanitario
Tipo di Dati **(Personale / Sensibile / Giudiziario)**	**P / S**
Personale che ha accesso ai dati	Medici, Infermieri, Coordinatrici di nucleo, Logopedisti, Fisioterapisti, Assistenti Sociali.
Modalità di raccolta	Manuale, con documenti e modulistica.
Modalità di trattamento	Informatico, cartaceo
Ambito di comunicazione	Ad uso interno, e ad uso dell'ULSS4.
Luogo in cui sono custoditi	Server ULSS4
Ubicazione (hardware)	ULSS4
Tipo di connessione ai dati	Via VPN, su rete proprietaria dell'ULSS4.
Misure di sicurezza adottate	Accesso protetto da password tramite autenticazione utente/password di sistema e utente di procedura (ciascun utente utilizza un proprio account/password). La password di accesso non è soggetta a cambiamento: dopo due minuti di inattività la postazione si blocca automaticamente, richiedendo nuovamente l'accesso con le credenziali.
Annotazioni	La gestione è affidata integralmente all'ULSS4, al quale ci si rivolge per la richiesta di attivazione di nuove utenze (tutte nominative) e per la comunicazione delle utenze da cessare.

Censimento Archivi : annotazioni

Finalità del trattamento:	es. finalità amministrativo-contabile, carattere sanitario, carattere sociale, altro…
Natura dei dati:	dati fiscali/contabili, dati normativi, dati famiglia, dati sindacali, dati sanitari, vita sessuale, altro…
Modalità di Raccolta dei dati:	come sono raccolti i dati: sportello, modulo, autocertificazione….
Modalità del trattamento:	trattamento cartaceo, informatico, videoregistrazione
Luogo in cui sono custoditi:	indicare il luogo fisico in cui sono ubicati gli archivi elettronici e cartacei
Ambito di comunicazione:	indicare i soggetti a cui sono comunicati i dati (enti locali, asl,, familiari, cooperative/associazioni, assicurazioni,altro…)
Misure di sicurezza e di protezione	dei dati attualmente in uso: chiusura a chiave, password…
Persone che hanno accesso ai dati:	indicare le Figure di incaricato. Ad esempio:

- 1)Medici e laureati non medici appartenenti al ruolo sanitario
- 2)Infermieri e tecnici ausiliari
- 3) Ausiliari
- 4) Amministrativi e tecnici che trattano dati sensibili o giudiziari
- 5) Amministrativi e tecnici che non trattano dati sensibili o giudiziari

5 AUTORIZZAZIONE ACCESSI INFORMATICI

5.1 Scopo

Lo scopo della procedura, art 34 D.Lgs 196/03, è quello di adottare un sistema di autorizzazione inteso come un insieme di strumenti e modalità che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente. Tale procedura ha quindi lo scopo di provvedere a quali aree o dati l'utente può accedere e una volta entrato quali azioni può compiere.

La finalità della procedura è quindi di definire modalità che consentano l'accesso agli strumenti elettronici solo a chi è autorizzato. Con tale procedura si verifica l'identità dell'utente abilitato al trattamento dei dati e si individuano delle procedure di gestione delle credenziali di autenticazione. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato ad una parola chiave riservata conosciuta solamente dal medesimo.

5.2 Campo Di Applicazione

Questa procedura, che concerne il sistema informatico aziendale, si applica a tutte le aree aziendali e per tutti i sistemi contenenti archivi dati (sia in rete sia stand-alone) della **Casa di Ricovero "Muzan"**.

I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai solo dati necessari per effettuare le operazioni di trattamento.

5.3 Responsabilità

La password è scelta e tenuta celata da ciascun utente.

Si ricorda che la **password** è personale e segreta.

La password deve avere una lunghezza minima pari almeno a otto caratteri e deve inoltre rispettare una serie determinati requisiti:
non deve contenere riferimenti riconducibili allo stesso incaricato (ad esempio nome, data di nascita, ecc.). E' consigliabile che ogni password contenga dati sia alfabetici che numerici;
Essere impostata dall'incaricato al primo utilizzo, essere mantenuta segreta e cambiata dallo stesso incaricato ogni sei mesi, ridotti a tre mesi nel caso che si trattano dati sensibili e giudiziari.

Non deve, inoltre, essere divulgata; nel caso in cui si abbia il sospetto che qualcuno possa esserne venuto a conoscenza è obbligatorio darne comunicazione al Preposto alla Custodia delle copie delle credenziali e farla cambiare immediatamente (Nella fattispecie è stato affidato al responsabile delle misure di sicurezza il ruolo di custode delle copie delle credenziali).

Periodicamente e almeno annualmente si deve verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

5.4 Riferimenti

DECRETO LEGISLATIVO 30 giugno 2003, n.196 Codice in materia di protezione dei dati personali

Art.33 (misure minime)
Art. 34 (Trattamenti con strumenti elettronici)
DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA

(Artt. da 33 a 36 del codice)

5.5 Contenuto

5.5.1 Procedure di accesso

Il sistema presenta un "prompt" di accesso che richiede e verifica la password unitamente allo "User ID", necessario per l'identificazione dell'utente e del profilo informatico (accesso, consultazione, possibilità di modifica dei dati degli archivi).

Per accedere alla rete aziendale è necessario avere:

Uno USER ID (assegnato dal Responsabile delle misure di sicurezza)
Una PASSWORD (privata e segreta)

5.6 Gestione user id

5.6.1 Creazione

Ogni Referente di area, al momento dell'inserimento di nuovo incaricato nella propria struttura o al momento di cambio di mansione del personale già presente, è tenuto a comunicare al Responsabile delle misure di sicurezza il nuovo profilo utente o la modifica di quello esistente.

E' infatti onere del Responsabile delle misure di sicurezza fissare i profili utente nel sistema informatico, anche in base alle indicazioni e disposizioni fornite dal Titolare del trattamento.

5.6.2 Disattivazione User ID

Lo User ID è disattivato e reso inutilizzabile dal Responsabile delle misure di sicurezza in caso si verifichino le seguenti condizioni:
inutilizzo dello stesso User ID per un periodo superiore a sei mesi;
uscita dall'azienda del dipendente.

Nel primo caso, il Responsabile delle misure di sicurezza controlla gli accessi con cadenza semestrale e, al sussistere della condizione, provvede a disattivare gli User ID e a registrare l'operazione.

Nel secondo caso, il Referente d'area comunica con tempestività l'uscita dall'azienda dell'utente in modo che il Responsabile misure di sicurezza possa rendere immediatamente inutilizzabile lo User ID.

5.6.3 Password

La password, personale e segreta, non deve essere divulgata e nel caso in cui si abbia il sospetto che qualcuno possa esserne venuto a conoscenza, è obbligatorio cambiarla immediatamente.

La lunghezza minima della password deve essere di otto caratteri, salvo l'ipotesi che gli strumenti non consentano una tale lunghezza per limiti del sistema. Non può, inoltre, essere riproposta una password già utilizzata in precedenza. La password deve avere una durata di massimo tre/sei mesi a seconda della tipologia di dati trattati allo scadere dei quali dovrà essere ridefinita e reimpostata dall'utente.

Per la definizione della password si tengano presenti i seguenti suggerimenti:
no riferimenti personali (nome, cognome, data di nascita ecc)
no solo lettere

5.6.4 Password per l'accesso al dominio e all'utilizzo delle risorse di rete (credenziali di autenticazione ed autorizzazione)

Per poter accedere alla rete ed utilizzare i vari applicativi e/o risorse gli incaricati dispongono delle seguenti password:

password di rete (utente in dominio per l'accesso alla rete aziendale);
password di accesso al software applicativo di CBA;
password per accedere alla rete remota di ESAKON (connessione remota);
password per accedere agli applicativi web di ESAKON (utente e password di procedura);
password per accedere alla posta elettronica.

5.6.5 Rilascio di una nuova password

Nel caso in cui un utente abbia dimenticato la password può richiederne la disattivazione al Responsabile delle misure di sicurezza. Tale procedura potrà essere autorizzata anche qualora vi sia la documentata necessità di accedere al sistema tramite la login dell'utente momentaneamente impossibilitato a farlo personalmente.
Dopo aver violato l'accesso disabilitando la password dell'utente, l'utente dovrà al più presto ridefinirne una nuova.

6 MISURE DI PROTEZIONE DELLA RETE AZIENDALE

6.1 Scopo

Scopo di questa procedura é garantire la gestione e l'aggiornamento di dotazioni protettive contro il rischio di intrusione ad opera di programmi di cui all'art.615-quinquies del codice penale come previsto dall'art.34 del D.Lgs. 196/03 e dal punto 16-17 del Disciplinare tecnico.

Fino a poco tempo fa le maggiori minacce alla sicurezza dei sistemi informativi erano costituite da floppy disk non identificati, password troppo facili da individuare, con l'avvento di Internet questi pericoli sono tuttavia diventati di "second'ordine", dal momento che la rete delle reti espone il sistema a tutta una nuova gamma di rischi potenziali contro i quali è essenziale predisporre misure di sicurezza di maggiore efficacia come software antivirus, antispam, Firewall, server Proxy.

6.2 Campo di Applicazione

Questa procedura concerne i sistemi di protezione adottati a livello aziendale, per proteggere la rete della **Casa di Ricovero "Muzan"** contro attacchi esterni.

Lo scopo della procedura è definire responsabilità e modalità operative per assicurare il corretto funzionamento delle misure di protezione e garantire la sicurezza dei dati personali e sensibili memorizzati sulla rete informatica.

6.3 Responsabilità

Il Titolare del trattamento predispone i mezzi necessari all'installazione ed al periodico aggiornamento del software antivirus e alla programmazione dei Firewall e Proxy in modo da assicurare che le policy siano rispettate.

6.4 Riferimenti

Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali
ALLEGATO B. DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (Artt. da 33 a 36 del codice)

LEGGE 23 dicembre 1993, n.547
Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica

6.5 Contenuto

Software Antivirus

L'intera rete aziendale è monitorata dal software Antivirus Trend Micro Worry-Free Business Security (client-server), installato sul server, e tramite apposito agent (Trend Micro OfficeScan) attivo sui vari client collegati in rete.

L'aggiornamento dei software antivirus è automatico e quotidiano.
L'amministratore di sistema, o il referente dell'azienda che si occupa della manutenzione hardware, aggiorna il software antivirus rendendo disponibile l'ultima versione.

Firewall

La connessione ad internet è garantita da accesso su linea ADSL fornita da NGI, su router LinkSys X3000, con regole su firewall Watchguard X550e, che gestisce gli accessi tenendo traccia dei contatti.

La gestione delle regole di sicurezza, del settaggio e della verifica del corretto funzionamento del sistema è gestita dal personale interno, in collaborazione con l'azienda esterna che cura l'intera struttura hardware (GPI Spa di Arzignano).

Non sono disponibili delle connessioni VPN per le aziende che forniscono servizi legati ai software installati, le quali operano in teleassistenza esclusivamente con software specifici, attivati dagli operatori interni on-demand.

Proxy

La connessione ad internet è autorizzata tramite sistema proxy GFIWebMonitor installato sul server.
Sono stati definiti tre diversi livelli di accesso:
Gruppo A : al personale che appartiene a questo gruppo è inibito qualsiasi accesso ad internet. La maggior parte degli utenti di dominio che non appartengono all'area amministrativa / sociale è iscritta in questo gruppo.
Gruppo B : al personale di questo gruppo sono stati resi accessibili solamente i siti istituzionali. A quest'area appartiene il personale medico e gli assistenti sociali.
Gruppo C : il personale amministrativo, normalmente iscritto in questo gruppo, ha la disponibilità per la piena navigazione.

Per ciascun utente sono stati comunque bloccati gli accessi ai siti "pericolosi" e ai social-network.
I log della navigazione sono conservati per 60 giorni, con registrazione delle informazioni specifiche del singolo utente.

6.6 Controllo

Dati in rete

Automaticamente, tutti i dati registrati nelle memorie di massa in rete sono sottoposti al controllo antivirus.

Dati in locale

I dati salvati sul disco fisso di ogni PC aziendale, sono sottoposti a controllo antivirus quotidianamente. L'attivazione del controllo è pianificata ed eseguita automaticamente da un apposito programma quando il PC è acceso.

Ogni utente può eseguire un controllo antivirus sul disco fisso del proprio PC al manifestarsi di fenomeni quali ad esempio:
messaggi diversi da quelli standard;
perdita di file o aumento del volume dei file;
rallentamento della velocità della macchina;
mancanza di spazio su disco;
impossibilità di accedere alle risorse di sistema;
in ambiente Office, malfunzionamenti nella gestione dei documenti o la presenza di macro in documenti che non ne prevedevano.

Se il controllo antivirus non risolve il problema o non evidenzia alcuna anomalia è necessario rivolgersi al Responsabile delle misure minime.
Non è consentito all'utente di disattivare il programma antivirus.
Tale operazione è consentita al solo Amministratore di sistema.

File di origine esterna

Ogni utente che riceva file di origine esterna, via E-mail o su altri tipi di supporto, è tenuto ad eseguire un controllo antivirus dei dati prima di utilizzarli, ed in particolare:

Chiavi USB, CD, sia quando sono dati all'esterno sia quando sono ricevuti, dovrebbero essere sottoposti al controllo antivirus;
tipicamente i virus si aggiungono ai file di programma quindi attenzione alla trasmissione e ricezione di file "eseguibili" *(.COM, .EXE, .OVL, .OVR, .DLL)* e di sistema *(.SYS)* anche tra computer in rete;
non utilizzare i server di rete come stazioni di lavoro;
non aggiungere mai dati o file a chiavi USB, CD, contenenti programmi originali

Log degli accessi

Il firewall mantiene registrazione solamente dei tentativi di accesso non autorizzato dall'esterno verso la rete aziendale.
Il sistema Proxy invece registra i dati della navigazione a livello utente, e viene mantenuto per una durata media di 6 mesi (sono salvati su server): le verifiche vengono effettuate sul traffico in entrata, al fine di analizzare i tentativi di accesso non autorizzato e di attacco alla rete.

7 GESTIONE BACKUP E PIANO DI DISASTER RECOVERY

7.1 Scopo

Lo scopo della procedura è definire le modalità e la frequenza di esecuzione delle copie di salvataggio dei dati e/o dei programmi residenti negli elaboratori strumentali all'attività aziendale.

L'utilizzo di tali copie è previsto nel caso di danneggiamento o perdita dei dati memorizzati su disco ed avviene attraverso procedure di ripristino e disaster-recovery.

7.2 Campo Di Applicazione

Questa procedura, che concerne il sistema informatico aziendale, si applica a tutti i dati contenuti negli elaboratori e nei supporti di memoria di massa della rete aziendale della **Casa di Ricovero "Muzan".**

La procedura di salvataggio, che può essere schedulata ed effettuata automaticamente, viene applicata a tutti gli archivi e programmi ritenuti critici dall'azienda indipendentemente dal sistema sul quale sono inclusi (vedi censimento archivi).

7.3 Responsabilità

Responsabile delle attività di "backup" è il Responsabile misure di sicurezza e/o eventuali incaricati precedentemente individuati.

E' compito del Titolare del trattamento dei dati o di un suo delegato, in collaborazione con il Responsabile del trattamento, individuare gli archivi contenenti i dati e mantenere aggiornato il relativo censimento.

7.4 Riferimenti

DECRETO LEGISLATIVO 30 giugno 2003, n.196 Codice in materia di protezione dei dati personali
Art.31 - Art. 34

DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA
(Artt. da 33 a 36 del codice)

7.5 Modalità di Salvataggio e Personale Incaricato

Sono stati inventariati i prodotti software acquisiti ed le rispettive tipologie di backup, che rendono possibili, in caso di problemi, le reinstallazioni; sono stati inoltre elencati i supporti di memorizzazione relativi ai salvataggi o copie, ed i relativi luoghi di conservazione.
Al fine di tutelare adeguatamente i dati gestiti nei vari sistemi di elaborazione è stato predisposto un adeguato piano di backup.

Nel prospetto che segue, si riepilogano le modalità di backup utilizzate.

Salvataggio				
Database	**Dati sensibili o giudiziari contenuti**	**Criteri individuati per il salvataggio**	**Ubicazione di conservazione delle copie**	**Struttura operativa incaricata del salvataggio**
Server 2012 (Gestionale CBA e Documenti Office Automation)	**Si (in parte)**	**Giornaliero** Giornalmente i documenti e i database residenti sul server vengono copiati (tramite Uranium Backup) sul NAS (Terastation) dislocato nell'ufficio amministrativo. **Mensile** Su base mensile poi viene effettuata una copia, sempre integrale su NAS. Al termine del backup viene generato un file di log, inviato via mail all'azienda che si occupa della manutenzione hardware. I supporti di norma vengono sostituiti solo in seguito a segnalazione di malfunzionamento della libreria.	**Terastation presso ufficio amministrativo**	**Automatico** **Personale Ufficio Amministrazione**
Sherpa (Gestionale)	**Si (in parte)**	I dati risiedono sui server di Esakon, a Trento, ai quali si accede tramite web.	**Esakon (Trento)**	**Esakon**
IATROS	**Si**	**Giornaliero** Il software prevede una copia dei dati dalla postazione in locale al server, tramite un batch automatico.	**Server 2012**	**Automatico**

7.6 Disaster Recovery

Non è previsto un effettivo piano di Disaster Recovery : i dati di backup sono a disposizione dei richiedenti in caso di perdita dei dati e/o malfunzionamenti dei sistemi informativi.
L'Amministratore di Sistema, su autorizzazione del Responsabile del trattamento, fornisce al richiedente i dati necessari relativi agli archivi a cui il richiedente ha accesso in condizioni normali.

Dovranno pertanto essere predisposte specifiche istruzioni operative al fine di consentire il corretto restore dei dati.

8 DATI PERSONALI TRATTATI ALL'ESTERNO DELL'ORGANIZZAZIONE

8.1 Generalità

In questa procedura viene fatto un quadro sintetico delle attività affidate a terzi che comportano il trattamento di dati, con l'indicazione sintetica del contesto giuridico o contrattuale (organizzativo e tecnico) in cui tale trasferimento si inserisce, in riferimento agli impegni assunti, anche all'esterno, per garantire la protezione dei dati stessi.

8.2 Scopo e Campo Di Applicazione

Lo scopo della procedura è individuare la tipologia di dati personali trasferiti all'esterno, i soggetti a cui vengono trasferiti i dati ed i criteri adottati dal Titolare per un adeguato trattamento.

8.3 Riferimenti Legislativi

Punto 19.7 DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA (Allegato B al D.lgs. 196/03)

8.4 Soggetti Esterni e Attività Esternalizzate

Di seguito sono riportate le attività effettuate all'esterno, che comportano trattamenti di dati personali, con l'indicazione dei soggetti a cui vengono trasferiti i dati:

Descrizione attività esternalizzata	Denominazione soggetti esterni	Sedi del trattamento
Società che effettua le elaborazioni mensili ed annuali relative al personale dipendente ed assimilato.	CBA S.p.A.	Trento
Studio Contabile (Commercialista) solo per dichiarazioni annuali e analisi di bilancio	Gruppo Consulenti Aziendali	Padova (PD)
Gestione Software contabilità, magazzino, Clienti – Fornitori, Gestione Ospiti. *(Connessione remota del personale della Casa di Ricovero "Muzan" ai server remoti)*	ESAKON S.n.c.	Volano (TN)
Assistenza Legale	Studio PERON CERA	Torri di Quartesolo (VI)
Medicina del lavoro (medico competente)	Dott. FELICE Gentile	Nove (VI)
Tesoreria, per pagamenti a fornitori ed incassi delle rette.	Cassa di Risparmio del Veneto	Agenzia di Malo (VI)
Gestione servizio operatori di cucina.	Cooperativa "MANO AMICA"	Schio (VI)
Gestione servizio pulizie	Serenissima Ristorazione S.p.A.	Vicenza (VI)
Agenzia Interinale per somministrazione lavoro (OSS e Ausiliari)	QUANTA S.p.A.	Vicenza (VI)
Medico di Medicina Generale in convenzione ULSS 4	Dott. SALVATO Giosuè	C/o Istituto
	Dott.ssa BONOLLO Sabrina	
	Dotto. TREVISAN Daniele	
Medici di Guardia Medica in convenzione ULSS 4	Dott. ZANIN Paolo	
	Dott. VERONESE Francesco	
	Dott.ssa SANTACATERINA Silvia	
Logopedista in convenzione ULSS 4	CAVEDON Francesca	
Servizio di Ristorazione (con Dietista)	Serenissima Ristorazione	Vicenza
Tirocinio Formativo	Università degli studi di Padova Facoltà di Medicina e Chirurgia	C/o Istituto
	Istituto professionale statale "Bartolomeo Montagna"	
	IPSIA "ANDREA SCOTTON"	
	ULSS4 (per infermieri)	
Revisori del Conto	CUNICO Andrea BEGHIN Giovanna DAL MOLIN Mirko	

8.5 Criteri di Garanzia del Trattamento

I criteri di garanzia adottati dal Titolare per un adeguato trattamento di dati effettuati da soggetti esterni

Soggetto	Descrizione criteri di garanzia di adeguato trattamento	Note
CBA S.p.A.	Nomina a responsabile esterno del trattamento dati.	
ESAKON S.n.c.	Nomina a responsabile esterno del trattamento dati.	La nomina è stata effettuata, e l'azienda ha fornito copia del loro DPS, nel quale sono dettagliate le misure di sicurezza utilizzate.
Gruppo Consulenti Aziendali	Nomina a responsabile esterno del trattamento dati.	
Cassa di Risparmio del Veneto		
Cooperativa "MANO AMICA"		
CAVEDON Francesca		
SERENISSIMA Ristorazione		
Dott. FELICE Gentile	Comunicazione al medico, certificandone la titolarità autonoma nel trattamento dei dati.	
Assistenza Legale	L'autorizzazione al trattamento di dati sensibili e dati giudiziari, esclusivamente ai fini dell'azione in giudizio o dell'esercizio di un diritto in sede giudiziaria, è consentita in virtù delle autorizzazioni standard del Garante per la protezione dei dati personali n. 4/2002 e n. 7/2002.	
Medici in convenzione con ULSS 4	I termini di riservatezza sono indicati nella convenzione.	
Revisore del Conto	Richiedere una attestazione di conformità al D.Lgs 196/2003 per trattamenti di dati personali effettuati.	
Aziende per Tirocinio Formativo	Gli impegni di riservatezza sono regolamentati dalle convenzioni con le varie strutture.	Agli stagisti, tirocinanti, ed alle altre figure inviate dalle Agenzie interinali che operano nella struttura, viene effettuata la nomina ad incaricato al trattamento, in base alle mansioni affidate a ciascuna figura professionale.
Agenzia Interinale per somministrazione lavoro		

Gli impegni di riservatezza sono regolamentati nel contratto di affidamento del servizio.
Inoltre l'Azienda ha richiesto a ciascun soggetto esterno di dichiarare:

1. di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali sono soggetti all'applicazione del codice per la protezione dei dati personali;
2. di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali
3. di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere.
4. di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze
5. di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

9 PROCEDURA GESTIONE INTERNET E POSTA ELETTRONICA

9.1 Scopo

Lo scopo della presente procedura è quello di definire le modalità per la richiesta e l'utilizzo di Internet e della Posta Elettronica della **Casa di Ricovero "Muzan".**

9.2 Campo di Applicazione

La procedura è rivolta a coloro che utilizzano Internet e il servizio di posta elettronica, sia a scopo di ricerca sia per promuovere attività commerciali utili per l'azienda.

9.3 Responsabilità

Il compito di emettere la richiesta di accesso a Internet è del Responsabile dell'Area.
Il compito di abilitare il servizio è del Responsabile delle misure minime di sicurezza.

9.4 Contenuto

L'Azienda accede ad Internet attraverso una linea ADSL protetta da firewall Watchguard e sistema proxy GFI WebMonitor.
La posta elettronica (Zimbra) è accessibile anche in modalità web mail, ed i server sono in hosting presso l'azienda che offre anche i servizi di manutenzione hardware (GPI Spa).

9.5 Abilitazione

La facoltà di utilizzo di Internet viene data agli utenti previa autorizzazione dal Titolare.
Tutte le operazioni necessarie all'abilitazione del collegamento vengono condotte esclusivamente dal Responsabile delle misure minime di sicurezza.

9.6 Utilizzo

Gli utenti abilitati possono accedere liberamente a Internet, successivamente all'autenticazione sulla postazione con utente e password di rete.

Ogni utente, come da accordi con lo staff di direzione, provvede direttamente alla modifica periodica della propria password.

L'amministratore di sistema interviene nei casi in cui sia necessario l'azzeramento di password ed è l'unico utente vincolato alla consegna delle buste con le proprie password d'accesso.

9.7 Misure di Sicurezza

Le misure minime di sicurezza contro infezioni e/o attacchi dall'esterno sono descritte nella procedura di "Autorizzazione accessi informatici", nella procedura "Gestione antivirus" (PGR01 e PGR02).

9.8 Riferimenti

Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali
Allegato b. disciplinare tecnico in materia di misure minime di sicurezza
Legge 23 dicembre 1993, n.547: modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica

Art. 113, 114 e 184, comma 3, del Codice; artt. 4 e 8 l. 20 maggio 1970, n. 300).
Art. 2, comma 5, Codice dell'amministrazione digitale
Del. n. 13 del 1° marzo 2007 del Garante della Privacy

9.9 Direttive Ministeriali e Linee Guida del Garante

Come ribadito inoltre dalla direttiva 02/2009 della Presidenza del Consiglio dei Ministri, Dipartimento della Funzione Pubblica, "*le Pubbliche Amministrazioni sono tenute ad assicurare la funzionalità ed il corretto impiego degli strumenti ITC da parte dei propri dipendenti, definendone le modalità di utilizzo nell'organizzazione dell'attività lavorativa ed adottando le misure necessarie a garantire la sicurezza, la disponibilità e l'integrità dei sistemi informativi*".
Si rammenta inoltre che, oltre alle disposizioni del Codice disciplinare contenuto nei contratti collettivi di comparto (che dispongono sanzioni in caso di negligenza nella cura dei locali, beni mobili o strumenti affidati sui quali, in relazione alle sue responsabilità , debba espletare azioni di vigilanza. Art. 25 CCNL 22/01/2004), anche il dettato del Codice di comportamento dei dipendenti delle pubbliche amministrazioni (di cui al Decreto del Ministero della funzione pubblica del 28/11/2000), dispone che il dipendente non debba utilizzare a fini privati materiale o attrezzature di cui dispone per ragioni di ufficio.
Pertanto l'utilizzo delle risorse ITC da parte dei dipendenti, oltre a non dover compromettere la sicurezza e la riservatezza del Sistema Informativo, non deve pregiudicare ed ostacolare le attività dell'Amministrazione, od essere destinato al perseguimento di interessi privati.
Conciliando quanto disposto dal Dipartimento di Funzione pubblica con quanto già definito nelle linee guida del Garante, il datore di lavoro ha la facoltà di controllare l'effettivo adempimento della prestazione lavorativa ed il corretto utilizzo degli strumenti di lavoro: il lavoratori per contro, devono essere posti in gradi di conoscere quali sono le attività consentite, quali i controlli attivi, le modalità di trattamento dei dati di analisi e le sanzioni nelle quali possono incorrere in caso di abuso.

9.10 Posta elettronica

Gli incaricati assegnatari delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.
Pertanto è vietato utilizzare le caselle di posta elettronica dell'Istituto per l'invio di messaggi personali o per la partecipazione a dibattiti, forum o mail list salvo diversa ed esplicita autorizzazione da parte del Responsabile di area.
È da evitare la divulgazione degli indirizzi destinati alla ricezione di comunicazioni ufficiali.
In caso di ricezione accidentale di messaggi di valenza ufficiale sulle caselle assegnate, gli assegnatari dovranno inoltrarli tempestivamente al responsabile delle misure minime di sicurezza.
Attraverso la rete interna dell'azienda non è consentita la consultazione di caselle di posta elettronica personali in nessuna forma, compreso l'accesso via browser

Posta elettronica interna

L'utilizzo della posta elettronica interna contribuisce fortemente a rendere la comunicazione tempestiva, efficace ed economica.
Il rispetto di alcune semplici regole può aiutare a migliorare ulteriormente l'utilizzo dello strumento:
La casella di posta assegnata deve essere mantenuta in ordine, cancellando i documenti inutili specialmente se contengono allegati ingombranti.
È buona norma riportare il soggetto mittente ed evitare messaggi completamente estranei al rapporto di lavoro.
Le politiche antivirus sono applicate anche alla posta interna.
È possibile utilizzare la ricevuta di ritorno per avere la conferma della avvenuta lettura del messaggio da parte del destinatario, ma si ricorda che per la comunicazione ufficiale è obbligatorio avvalersi degli strumenti tradizionali (fax, posta, …).

Per la trasmissione di file all'interno della stessa sede è preferibile l'utilizzo delle unità di rete piuttosto che allegare il documento ad un messaggio di posta elettronica

Posta elettronica esterna

La posta elettronica proveniente dall'esterno viene ricevuta direttamente sul PC dell'incaricato, quindi analizzata da un antivirus.

9.11 Posta elettronica e assenza del lavoratore

In caso di assenze (per ferie o attività di lavoro fuori sede) è predisposto un sistema di invio automatico di messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o di un'altra area della struttura. I lavoratori sono tenuti ad avvalersi di tali modalità, prevenendo così l'apertura della posta elettronica.
In caso di eventuali assenze non programmate (ad es. per malattia), qualora il lavoratore non possa attivare la procedura sopra descritta, il titolare del trattamento, perdurando l'assenza oltre un determinato limite temporale, può disporre, se necessario, mediante personale appositamente incaricato (ad es. l'amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati), l'attivazione di un analogo accorgimento, avvertendo gli interessati.
Qualora si debba conoscere il contenuto dei messaggi di posta elettronica per improrogabili necessità legate all'attività lavorativa, in caso di assenza improvvisa o prolungata, l'interessato dovrà delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell'attività lavorativa.
Tale fiduciario è stato individuato dall'azienda nella persona del Responsabile dell'area di riferimento, e in caso di sua assenza nel Responsabile CED, su richiesta della Direzione.

9.12 Utilizzo della rete Internet e dei relativi sevizi

Le reti telematiche pubbliche o "aperte" (come Internet) contengono una pluralità di porte di ingresso che immettono in siti di libero accesso e in siti privati (come le caselle della posta elettronica) o a pagamento.
L'utilizzo imprudente di alcuni servizi della rete Internet può essere fonte di minacce alla sicurezza e all'immagine consortile.

Operazioni vietate durante la Navigazione Internet

È da evitare il download di programmi software, anche gratuiti, se non per esigenze strettamente professionali, fatti salvi i casi di esplicita autorizzazione del responsabile delle misure minime di sicurezza. Qualora fosse stata fatta qualche installazione non consentita, l' utilizzatore del personal computer deve avvertire il responsabile delle misure minime di sicurezza, affinché possa procedere alla immediata disinstallazione del software.
È da evitare ogni forma di registrazione a siti i cui contenuti non siano strettamente legati all'attività lavorativa.
È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

9.13 Controllo delle informazioni

Vengono memorizzati temporaneamente, per un mese, ai soli fini della sicurezza aziendale, informazioni quali file di log.
Normalmente accedono solo in caso di necessità gli incaricati alla manutenzione della rete, ai soli fini della sicurezza aziendale.
Vengono conservati in forma centralizzata i dati di backup della posta elettronica aziendale, per ragioni organizzative e produttive al fine di recuperare i dati in caso di perdita da parte degli utenti interessati .
E' stato predisposto un sistema di filtri su suite antivirus al fine di prevenire operazioni ritenute incoerenti con l'attività lavorativa (accesso a determinati siti, download di file o software aventi particolari caratteristiche)
Il titolare del trattamento si riserva di effettuare controlli saltuari in conformità alla legge, per verificare la funzionalità e sicurezza del sistema
Il trattamento dei dati (es file di log) è effettuato in forma anonima o in modo tale da precludere l'immediata identificazione di utenti (es tramite opportune aggregazioni)

In caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni
Saranno prese conseguenze, anche di tipo disciplinare, qualora venga constatato che la posta elettronica e la rete Internet sono utilizzate indebitamente.

9.14 Ulteriori controlli

Non sono attivi ulteriori controlli sul traffico e sulla rete.

10 ATTRIBUZIONE DELLE FUNZIONI DI AMMINISTRATORE DI SISTEMA

10.1 Generalità

In questa procedura vengono descritti i compiti che il Titolare del trattamento ha affidato all'amministratore di sistema interno o esterno all'azienda.
Tali attività, possono comportare elevate criticità rispetto alla protezione dei dati, per cui risulta fondamentale individuare tali soggetti e le loro mansioni all'interno della struttura aziendale, e andarne a verificare con cadenza annuale la rispondenza.

10.2 Scopo e Campo di Applicazione

Lo scopo della procedura è individuare i soggetti che ricoprono il ruolo di amministratore di sistema presso della **Casa di Ricovero "Muzan"**; i compiti loro affidati; i criteri adottati dal Titolare nella scelta di tali figure; la registrazione degli access log ai sistemi di elaborazione e agli archivi elettronici, anche ai fini della verifica annuale.

10.3 Riferimenti Legislativi

DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA
(Allegato B al D.lgs. 196/03)

Provvedimento del 27/11/08 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"

10.4 Soggetti Esterni e Compiti Affidati

Di seguito sono riportate i soggetti esterni a cui è stato affidato dall'azienda una determinata attività inerente il sistema informativo aziendale, e la modalità con cui viene svolta.

Soggetto esterno	Attività affidata all'esterno	Modalità trattamento
CBA Spa Trento	Gestione software pacchetto CBA	Teleassistenza ed interventi presso l'azienda.
ESAKON Snc Volano (TN)	Gestione software pacchetto ESAKON	Teleassistenza.
GPI S.p.A. Arzignano(VI)	Manutenzione harware e gestione della rete	Teleassistenza ed interventi presso l'azienda.

Si allega elenco delle persone fisiche che i singoli soggetti esterni utilizzano per espletare gli impegni assunti con l'azienda, sia presso azienda sia in teleassistenza.

Soggetto esterno	Persone fisiche autorizzate ad effettuare gli interventi sia in azienda che in remoto, per conto del soggetto esterno
CBA Spa Trento	La nomina non è mai stata effettuata.
ESAKON Snc Volano (TN)	*La nomina è stata effettuata il 26/04/2010: il 26/04/2010 la società ha comunicato i nominativo degli AdS, ovvero PAROLARI Italo e BETTA Roberto.*
GPI S.p.A. Arzignano(VI)	*La nomina è stata effettuata il 22/02/2010: il 23/02/2010 la società ha comunicato il nominativo dell'AdS, ovvero BERTOLDO Matteo.*

10.5 Soggetti Interni e Compiti Affidati

Ad oggi non sono presenti nell'Istituto figure tali da essere inquadrabili nella mansione di "Amministratore di Sistema".
Attualmente il Direttore opera come front-end per la risoluzione di problematiche legate al sistema informatico, prima di inoltrare la richiesta di intervento all'azienda che si occupa della manutenzione dei sistema informatico aziendale (GPI Spa).

10.6 Registrazione degli Accessi

I dati degli accessi sono memorizzati nel registro eventi di windows del server di dominio, ed elaborati dal software GFI EventManager 11: la configurazione impostata è pari a quanto previsto dal Garante nel provvedimento specifico.

10.7 Verifica Annuale da Parte del Titolare del Trattamento

Il Titolare del trattamento è tenuto ad ottemperare all'obbligo di verifica annuale sull'attività svolta dai soggetti esterni e interni all'azienda.

11 GESTIONE DEGLI IMPIANTI DI VIDEOSORVEGLIANZA

11.1 Scopo

Scopo di questa procedura è di garantire che l'utilizzo di impianti di videosorveglianza per fini di sicurezza e di monitoraggio degli accessi sia effettuato nel rispetto del D.Lgs. 196/2003 "Codice sulla Privacy" e delle regole indicate dall'Autorità Garante per la Privacy. (Provvedimento sulla videosorveglianza del 8 aprile 2010).

11.2 Campo di Applicazione

La presente procedura si applica relativamente all'utilizzo degli impianti di videosorveglianza della **Casa di Ricovero "Muzan"** dislocati presso le sedi aziendali, i depositi, gli approdi, sui mezzi di trasporto.

11.3 Responsabilità

Il Titolare del trattamento è responsabile della definizione delle modalità di trattamento di informazioni raccolte mediante apparecchiature di videosorveglianza.

11.4 Definizioni

Per dato personale si intende "qualunque informazione relativa a persona fisica, a persona giuridica, ente o associazione identificati o identificabili, anche indirettamente mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale". Anche **immagini** o suoni sono dati personali, qualora le apparecchiature che li rilevano permettano di identificare, in modo diretto o indiretto, i soggetti interessati.
Per Incaricato si intende la "persona fisica autorizzata a compiere operazioni di trattamento dal Titolare o dal Responsabile".
Per **videocontrollo** si intende un sistema o dispositivo che permette la visione unicamente in tempo reale di aree o zone delimitate.
Per **videocitofoni** si intendono sistemi o dispositivi installato in corrispondenza di campanelli o citofoni per finalità di controllo dei visitatori che richiedono l'autorizzazione o si accingono ad entrare.
Per impianti di **videosorveglianza** si intende l'installazione di sistemi, reti ed apparecchiature che permettono la visione, ripresa e la registrazione di immagini, su supporti singoli, abbinati ad altre fonti o conservati in banche dati di immagini di aree o zone delimitate, in particolare a fini di sicurezza, di tutela del patrimonio, di controllo di determinate aree e di monitoraggio del traffico o degli accessi.
Con il termine poi di **Centrale di Videocontrollo e/o Videosorveglianza** si intende un sistema centrale dove sono convogliate ed eventualmente registrate le riprese effettuate dai dispositivi periferici.

11.5 Modalità Operative

L'azienda dispone di un sistema di monitoraggio, automatico 24 ore su 24, con 8 videocamere installate in quest'ordine:

- 3 postazioni poste esternamente all'ingresso di ciascun stabile (CDR, RSA e Veletta);
- 1 postazione internamente alla struttura RSA;
- 2 postazioni esterne nel lato opposto all'ingresso dello stabile RSA;
- 2 postazioni interne, in prossimità dell'ingresso, allo stabile RSA.

Il sistema di videosorveglianza prevede la registrazione su hard-disk : le immagini registrate sono conservate nella'hard-disk per la durata media di 52 ore, trascorse le quali vengono soprascritti.
Le registrazioni sono accessibile tramite software installato sulle postazioni del Direttore e della Responsabile servizi amministrativi.
Sono attivi due monitor di sola visualizzazione (on-line) posti nella cucinetta al piano terra della CDR e al 3° piano della RSA.
I dati raccolti non possono essere utilizzati per finalità diverse o ulteriori rispetto a quelle relative alla sicurezza, fatte salve le esigenze di polizia o di giustizia. I dati raccolti non possono essere diffusi o comunicati a terzi.

Le riprese sono tali da consentire visioni panoramiche evitando immagini particolareggiate e invasive della riservatezza delle persone.

La zona di ripresa è segnalata mediante cartelli che informano della presenza dell'impianto.

Nessuna telecamera riprende in modo stabile le postazioni di lavoro nel rispetto nei limiti stabiliti dallo Statuto dei Lavoratori.

La manutenzione dell'impianto è affidato al Gruppo Sicura Srl, di Vicenza, che opera su supervisione del sig. Marco Bernabè.

NB: alla data di stesura del documento, delle 8 videocamere installate 4 risultano non funzionanti. Dal momento che il sistema di registrazione prevede la memorizzazione delle immagini con modalità *on-motion*, la durata della registrazione è maggiore rispetto a quanto previsto (indicativamente sulle 78 ore).
L'impianto è comunque in via di revisione, in conseguenza della ristrutturazione in atto.
Si sta inoltre valutando di ampliare l'impianto, con l'installazione di ulteriori punti di ripresa nei corridoi dei 3 nuclei RSA, per motivi di sicurezza e protezione (sono occorsi di recente alcuni casi di furti a danno dei residenti).

11.6 Riferimenti

Provvedimento generale del 8 aprile 2010 del Garante per la protezione dei dati personali.

12 REGOLAMENTO PER IL TRATTAMENTO DI DATI SENSIBILI E GIUDIZIARI.

12.1 Premessa

Gli articoli 20, comma 2, e 21, comma 2, del decreto legislativo 30 giugno 2003, n. 196 stabiliscono che nei casi in cui una disposizione di legge specifichi la finalità di rilevante interesse pubblico, ma non i tipi di dati sensibili e giudiziari trattabili ed i tipi di operazioni su questi eseguibili, il trattamento è consentito solo in riferimento a quei tipi di dati e di operazioni identificati e resi pubblici a cura dei soggetti che ne effettuano il trattamento, in relazione alle specifiche finalità perseguite nei singoli casi.

Il medesimo art. 20, comma 2, prevede inoltre che detta identificazione debba essere effettuata nel rispetto dei principi di cui all'art. 22 del citato Codice, in particolare, assicurando che i soggetti pubblici :

- trattino i soli dati sensibili e giudiziari indispensabili per le relative attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa;
- raccolgano detti dati, di regola, presso l'interessato;
- verifichino periodicamente l'esattezza, l'aggiornamento dei dati sensibili e giudiziari, nonché la loro pertinenza, completezza, non eccedenza ed indispensabilità rispetto alle finalità perseguite nei singoli casi;
- trattino i dati sensibili e giudiziari contenuti in elenchi, registri o banche di dati, tenuti con l'ausilio di strumenti elettronici, con tecniche di cifratura o mediante l'utilizzazione di codici identificativi o di altre soluzioni che li rendano temporaneamente inintelligibili anche a chi è autorizzato ad accedervi;
- conservino i dati idonei a rivelare lo stato di salute e la vita sessuale separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo;

12.2 Testo del Regolamento

Attualmente la Casa di Ricovero non ha ancora adottato alcun testo di regolamento, avvalendosi pertanto del Regolamento Regionale del 22/03/2007 (Regione Veneto), pubblicato nel BUR n.31 del 27/03/2007.
La Direzione sta valutando l'ipotesi di adottare un apposito documento più corrispondente ai trattamenti effettuati nella Casa di Ricovero, da approvare come "*Regolamento per il trattamento di dati sensibili e giudiziari*" : il documento sarà poi allegato al DPS, nelle successive revisioni.